



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,802	01/09/2004	Hoe-Won Kim	678-1131	1597

66547 7590 06/19/2007  
THE FARRELL LAW FIRM, P.C.  
333 EARLE OVINGTON BOULEVARD  
SUITE 701  
UNIONDALE, NY 11553

EXAMINER
----------

PALIWAL, YOGESH

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

06/19/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/754,802	<b>Applicant(s)</b> KIM, HOE-WON	
	<b>Examiner</b> Yogesh Paliwal	<b>Art Unit</b> 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 09 January 2004.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 January 2004 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Priority***

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

### ***Drawings***

2. The drawings are objected to because of following informalities:
  - The block represented by figure 1 numeral 160 should read "Ks enciphering unit".
  - Figure 1 is not of sufficient quality, some of the details are hard to read, for example, encrypted data/key, going from numeral 140 (Transmitting/Receiving unit) to numeral 50 (Public network) is represented with alphabets, which are hard to read (especially the lower subscripts). Same is true for the data/key going from numeral 50 (public network) to numeral 200 (Security deciphering module).
  - Figure 4, numeral "480" should be replaced with numeral "490".

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet,

and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### ***Specification***

3. The disclosure is objected to because of the following informalities:
  - On page 7 line 20, "personal secret key {ks} Kh generated...", should read "personal secret key ({Ks} Kh) generated...". [Note: throughout the specification, inconsistency for using representation for enciphered data and personal secret key are found. In some instances enciphered data is represented "{M}Ks" and in some instances it is represented "{M}Ks", same is true for the representation of personal secret key throughout the specification. To avoid confusion, applicant needs to choose one representation for same element throughout the whole disclosure.]
  - On Page 9, line 14-15, delete the following line: "[PLEASE CORRECT FIG. 1 AS SHOWN.]".

- On Page 12, line 2, delete the following line: "[PLEASE CORRECT FIG. 3 AS SHOWN."].

Appropriate correction is required.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-10 are rejected under 35 U.S.C. 102(b) as being anticipated by

Akiyama et al. (US 2003/0002680 A1), hereinafter Akiyama.

- Regarding **Claim 1**, Akiyama discloses a security deciphering apparatus comprising (Fig. 14):

a hidden secret key storing unit for storing a hidden secret key (Kh)

corresponding to intrinsic identification information (**Fig. 14, Numeral 505, "Master Key Storage Unit (Km)"**);

a first decoding unit for receiving via a public network a personal secret key ([Ks]Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ([Ks]Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks) (**Paragraph 0108, "The reception device provided at each user's home receives the encrypted appending information**

**([Appending] Km) and decrypt it using the master key Km provided in that reception device”, Note: appending information contains a channel key Kch) and**

a second decoding unit for receiving via the public network enciphered data ([M]Ks), generated by enciphering data (M) by using the cipher key (Ks) **(Paragraph 0107, The broadcast station 200 broadcasts contents information ([Contents] Kch) which is encrypted using a channel key Kch”), and**

decoding the enciphered data ([M]Ks) by using the cipher key (Ks), thereby obtaining the data (M) **(Paragraph 0108, “...Channel key Kch contained therein is stored into a database provided in that reception device and will be used in decrypting the encrypted contents information ([Contents] Kch)”)**

Regarding **Claim 2**, Rejection of claim 1 is incorporated and further Akiyama discloses:

a personal secret key storing unit for storing the personal secret key ([Ks]Kh) received via the public network **(Fig. 14, Numerals 503 “Filter”)** and

outputting the stored personal secret key ([Ks]Kh) to the first decoding unit under a control of the first decoding unit **(Paragraph 0108, “The reception device provided at each user’s home receives the encrypted appending information ([Appending] Km) and decrypts it using the master key Km provided in that reception device”); and**

Art Unit: 2135

a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit (**Paragraph 0108, "...the channel key Kch contained therein is stored into a database provided in that reception device), and**

outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit (**Paragraph 0108, "... the channel key Kch contained therein is stored into a database provided in that reception device and will be used in decrypting the encrypted contents information ([Contents] Kch)"**).

Regarding **Claim 3**, Akiyama discloses a data service providing apparatus for providing data requested by a communication terminal (**Fig. 3**), comprising:

a data database for storing data (M) to be provided to the communication terminal (**Paragraph 0107, "The broadcast station 200 broadcasts contents information"**);

a hidden secret key database for storing a hidden secret key (Kh) corresponding to intrinsic identification information of a security deciphering module equipped in the communication terminal to decipher enciphered data (**Fig. 3, Numeral 10 and 3**)

a transmitting/receiving unit for performing communication with the communication terminal via a public network (**Fig. 3, Numeral 13**);

a data enciphering unit for enciphering the data (M) by using a cipher key (Ks) (**Paragraph 0107, "The broadcast station 200 broadcasts contents information ([Contents] Kch) which is encrypted using a channel key Kch"**) ;

Art Unit: 2135

a cipher key enciphering unit for enciphering the cipher key (Ks) by using the hidden secret key (Kh) (**Paragraph 0107, "...appending information ([Appending] Km) which is containing a terminal ID, a channel key Kch, etc. and encrypted using a master key Km"**); and

a control unit for controlling the enciphering operations of the data and cipher key enciphering units (**Fig. 3, Numerals 2, 1, 7, and 6**), and

controlling the transmitting/receiving unit to provide the enciphered data ([M]Ks) and the personal secret key ([Ks]Kh) via the public network (**Fig. 3, Numeral 14 "Scheduling Unit"**).

Regarding **Claim 4**, the rejection of claim 3 is incorporated and further Akiyama discloses that security deciphering module (Paragraph 0108, "The reception device") comprises:

a hidden secret key storing unit for storing the hidden secret key (Kh) corresponding to the intrinsic identification information of the security deciphering module (**Fig. 14, Numeral 505, "Master Key Storage Unit (Km)"**);

a first decoding unit for decoding the personal secret key ([Ks]Kh) provided by the transmitting/receiving unit, by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks) (**Paragraph 0108, "The reception device provided at each user's home receives the encrypted appending information ([Appending] Km) and decrypt it using the master key Km provided in that reception device", Note: appending information contains a channel key Kch**); and



a second decoding unit for decoding the enciphered data ([M]Ks) provided by the transmitting/receiving unit (**Paragraph 0107, The broadcast station 200 broadcasts contents information ([Contents] Kch) which is encrypted using a channel key Kch**”), by using the cipher key (Ks), thereby obtaining the data (M) (**Paragraph 0108, “...Channel key Kch contained therein is stored into a database provided in that reception device and will be used in decrypting the encrypted contents information ([Contents] Kch)”**).

Regarding **Claim 5**, the rejection of claim 4 is incorporated and further Akiyama discloses that the security deciphering module further comprises:

a personal secret key storing unit for storing the personal secret key ([Ks]Kh) provided by the transmitting/receiving unit (**Fig. 14, Numerals 503 “Filter”**), and

outputting the stored personal secret key ([Ks]Kh) to the first decoding unit under a control of the first decoding unit (**Paragraph 0108, “The reception device provided at each user’s home receives the encrypted appending information ([Appending] Km) and decrypts it using the master key Km provided in that reception device”**);, and

a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit (**Paragraph 0108, “...the channel key Kch contained therein is stored into a database provided in that reception device**),, and

outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit (**Paragraph 0108, “... the channel key Kch contained**

Art Unit: 2135

therein is stored into a database provided in that reception device and will be used in decrypting the encrypted contents information ([Contents] Kch)").

Regarding **Claim 6**, Akiyama discloses a security deciphering method comprising the steps of:

determining whether or not a personal secret key ([Ks]Kh), generated by enciphering a cipher key (Ks) by using a hidden secret key (Kh) corresponding to intrinsic identification information, is received (**Paragraph 0198, "When it is Judged that the entered packet contains the appending information according to the flag of that packet, this packet is added to the buffer for the appending information"**);

if it is determined that the personal secret key ([Ks]Kh) is received, then decoding the received personal secret key ([Ks]Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks) (**Paragraph 0108, "The reception device provided at each user's home receives the encrypted appending information ([Appending] Km) and decrypts it using the master key Km provided in that reception device"**);

determining whether or not enciphered data ([M]Ks), generated by enciphering data (M) requested to be transmitted by using the cipher key (Ks), is received (**Paragraph 0195, "Each packet has a flag information that enables to distinguish whether that packet is a packet containing the master key seed, a packet containing the appending information, or a packet containing the contents information."**);

and if it is determined that the enciphered data ([M]Ks) is received, then decoding the enciphered data ([M]Ks) by using the cipher key Ks, thereby obtaining the data (M) **(Paragraph 0188, "the contents information of the corresponding channel can be properly decrypted using the generated channel key Kch.")**

Regarding **Claim 7**, Akiyama discloses a data service providing method for providing data requested by a communication terminal, comprising the steps of:

receiving via a public network a request (Fig. 2, "Subscription") for transmission of data (M) from the communication terminal (Fig. 2);

enciphering the data (M) by using a cipher key (Ks) in response to the received data transmission request, thereby generating enciphered data ([M]Ks) **(Paragraph 0107, "The broadcast station 200 broadcasts contents information ([Contents] Kch) which is encrypted using a channel key Kch")**;

enciphering, in response to the received data transmission request, the cipher key (Ks) by using a hidden secret key (Kh) corresponding to intrinsic identification information assigned to a security enciphering module equipped in the communication terminal to decode the enciphered data ([M]Ks), thereby generating personal secret key ([Ks]Kh) **(Paragraph 0107, "...appending information ([Appending] Km) which is containing a terminal ID, a channel key Kch, etc. and encrypted using a master key Km")**; and

transmitting the enciphered data ([M]Ks) and the personal secret key ([Ks]Kh) to the communication terminal via the public network **(Fig. 3, Numeral 13, also at**

**Paragraph 0108, “The reception device provided at each user’s home receives the encrypted appending information ([Appending] Km) and decrypt it using the master key Km provided in that reception device”, Note: appending information contains a channel key Kch and at Paragraph 0108, “... the channel key Kch contained therein is stored into a database provided in that reception device and will be used in decrypting the encrypted contents information ([Contents] Kch)” );**

Regarding **Claim 8**, rejection of claim 7 above is incorporated and further Akiyama discloses, that the security enciphering module equipped in the communication terminal comprises **(Fig. 14):**

a hidden secret key storing unit for storing the hidden secret key (Kh) corresponding to the intrinsic identification information assigned to the security enciphering module **(Fig. 14, Numeral 505, “Master Key Storage Unit (Km)”);**

a first decoding unit for decoding the personal secret key ([Ks]Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks) **(Paragraph 0108, “The reception device provided at each user’s home receives the encrypted appending information ([Appending] Km) and decrypt it using the master key Km provided in that reception device”, Note: appending information contains a channel key Kch);** and

a second decoding unit for decoding the enciphered data ([M]Ks) **(Paragraph 0107, The broadcast station 200 broadcasts contents information ([Contents] Kch) which is encrypted using a channel key Kch”)** by using the obtained cipher key

Art Unit: 2135

(Ks), thereby obtaining the data (M) **(Paragraph 0108, "...Channel key Kch contained therein is stored into a database provided in that reception device and will be used in decrypting the encrypted contents information ([Contents] Kch)").**

Regarding **Claim 9**, rejection of claim 8 above is incorporated and further Akiyama discloses that the security deciphering module further comprises:

a personal secret key storing unit for storing the personal secret key ([Ks]Kh) received by the communication terminal via the public network **(Fig. 14, Numerals 503 "Filter")**, and

outputting the stored personal secret key ([Ks]Kh) to the first decoding unit under a control of the first decoding unit **(Paragraph 0108, "The reception device provided at each user's home receives the encrypted appending information ([Appending] Km) and decrypts it using the master key Km provided in that reception device")**; and

a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit **(Paragraph 0108, "...the channel key Kch contained therein is stored into a database provided in that reception device)**, and

outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit **(Paragraph 0108, "... the channel key Kch contained therein is stored into a database provided in that reception device and will be used in decrypting the encrypted contents information ([Contents] Kch)").**

Regarding **Claim 10**, Akiyama discloses in a mobile communication terminal receiving, via a public network, enciphered data ([M]Ks) generated by enciphering data (M) by using a cipher key (Ks), a security deciphering apparatus comprising:

a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information assigned to the mobile communication terminal (**Fig. 14, Numeral 505, "Master Key Storage Unit (Km)"**),  
Note: The reception device of Akiyama can be interpreted as mobile reception device, because at paragraph 10, Akiyama establishes that "this requirement is very hard to satisfy in the broadcasting service with respect to mobile reception devices which is expected to be associated with a poor reception state, a short reception time and a narrow bandwidth" and later in the specification at paragraph 0486, Akiyama establishes that "As described above, according to the present invention, it is possible to realize the conditional access while maintaining the same level of safety even when the broadcast bandwidth available to transmission of information related to the conditional access is narrow...", thus proving that his system would work for mobile reception device as well.);

a first decoding unit for receiving a personal secret key ([Ks]Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ([Ks]Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks) (**Paragraph 0108, "The reception device provided at each user's home receives the encrypted appending information ([Appending] Km) and**

**decrypt it using the master key  $K_m$  provided in that reception device”, Note:  
appending information contains a channel key  $K_{ch}$ ); and**

**a second decoding unit for decoding the enciphered data ( $[M]K_s$ ) (Paragraph 0107, The broadcast station 200 broadcasts contents information ( $[Contents] K_{ch}$ ) which is encrypted using a channel key  $K_{ch}$ ”) by using the obtained cipher key ( $K_s$ ), thereby obtaining the data ( $M$ ) (Paragraph 0108, “...Channel key  $K_{ch}$  contained therein is stored into a database provided in that reception device and will be used in decrypting the encrypted contents information ( $[Contents] K_{ch}$ ”).**

### ***Conclusion***

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

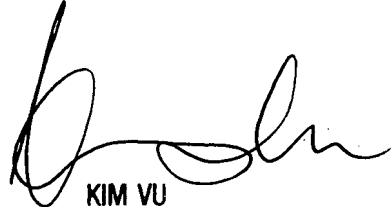
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

YP

6/5/2007



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2107